UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,267	03/31/2004	John P. Brizek	P18413/1020P18413	9827

57035 7590 12/22/2009

KACVINSKY LLC
C/O INTELLEVATE
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER	
PAN, JOSEPH T	
ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
12/22/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/816,267	BRIZEK ET AL.	
	Examiner	Art Unit	
	JOSEPH PAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 October 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-9,11-15,17-20 and 22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-9,11-15,17-20 and 22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's response filed on October 7, 2009 has been fully considered. Claims 1, 3-9, 11-15, 17-20 and 22 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-9, 11-15, 17-20 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al. (U.S. Patent No. 7,069,439 B1), hereinafter "Chen", in view of Nakayama et al. (U.S. Pub. No. 2004/0147251 A1), hereafter "Nakayama", and further in view of Hino et al. (U.S. Pat. No. 7,424,611 B2), hereinafter "Hino".

Referring to claims 1, 7, 15, 20:

i. Chen teaches:

A method, comprising:

dynamically generating a first set of integrity information for a first processing system by generating said first set of integrity information for an application using a cryptographic algorithm, the first processing system comprising a first processor (see figure 5, elements 530 'generate digest', 570 'compare metrics'; column 4, line 59-column 5, line 2; column 8, lines 4-16; and column 11, lines 5-16 of Chen);

sending said first set of integrity information to a second processing system, the second processing system comprising a second processor (see figure 5, elements 535 'sign & return digest' of Chen); and

generating an attestation value for said first processing system by said second processing system using said first set of integrity information and a dynamic attestation module connected to said second processing system prior to execution of said application by said first processing system (see column 11, lines 5-16, '...compares the computed integrity metrics, which it extracts from the challenge response, with the proper platform integrity metric, which it extracts from the certificate.'; and figure 5, element 590 'establish secure communication', of Chen, emphasis added).

Chen discloses dynamic authentication of the platform and application (see column 8, lines 4-16, particularly "Other know processes, for example virus checkers, will typically be in place to check that the operating system and **application program** code has not been subverted", of Chen, emphasis added). However, Chen does not specifically mention selecting an application from a plurality of applications.

Chen discloses generating set of integrity information for a processing system during boot operation (see column 7, lines 19-21 'During the secure boot process, the trusted device 24 acquires an integrity metric of the computing platform 10.', of Chen). However, Chen does not specifically mention the processing system that has completed trusted boot operation to verify integrity of an application prior to execution of the application.

Chen discloses terminating the session by the trusted device in case of an error or failure occurs (see column 13, lines 30-31, of Chen). However, Chen does not specifically mention disabling access by the processing system to a transceiver of the device.

ii. Nakayama teaches a portable terminal wherein Nakayama discloses selecting an application from a plurality of applications (see figure 5, element 222 'service identifier area' [i.e., a plurality of applications]; page 7, paragraph [0102], lines 9-12 "The service identifier area 222 stores identifiers of services (e.g., "0001",

"0002", "0003",...) for which the corresponding value entities in the value entity area 221 are used"; and paragraph [0098], lines 7-9 "or pull-type transmission in which the store server 30 transmits the application in response to an active transmission request from the portable terminal 20", of Nakayama).

Nakayama further discloses the transceiver (see page 6, paragraph [0087], lines 7-10, of Nakayama).

On the other hand, Hino teaches a authentication system wherein Hino discloses the processing system that has completed trusted boot operation to verify integrity of an application prior to execution of the application (see column 2, lines 5-11 'Authentication may be performed during any period when inoperativeness of unauthenticated programs is guaranteed. Therefore, the authenticator accepting period is not limited to a boot period which will be described below. That is, authentication is not limited within a period starting from generation of a system reset, and not limited within a period ending at activation of an OS.'; and column 3, lines 37-59, of Hino, emphasis added).

Hino further discloses a hardware having a disabling and an enabling functionality (see column 3, lines 60-63, of Hino).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Nakayama into the method of Chen to select an application from a plurality of applications for authentication.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Hino into the method of Chen to use the processing system that has completed trusted boot operation to verify integrity of an application prior to execution of the application.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Nakayama into the system of Chen to select an application from a plurality of applications for authentication, because Chen teaches dynamic authentication of platform and applications (see column 8, lines 4-16 of Chen), and Nakayama teaches selection an application from a plurality of applications (see ii

above). Therefore, Nakayama's teaching could enhance Chen's system by providing more flexibility.

The ordinary skilled person would have been motivated to have applied the teaching of Hino into the system of Chen to use the processing system that has completed trusted boot operation to verify integrity of an application prior to execution of the application, because Chen teaches dynamic authentication of platform and applications (see column 8, lines 4-16 of Chen), and Hino teaches using the processing system that has completed trusted boot operation to verify integrity of an application prior to execution of the application. Therefore, Hino's teaching could enhance Chen's system by providing security.

Referring to claims 3, 22:

Chen, Nakayama, and Hino teach the claimed subject matter: a method for performing dynamic attestation (see claim 1 above). Chen further discloses:

retrieving a second set of integrity information for said first processing system (see column 11, lines 5-16, '...compares the computed integrity metrics, which it extracts from the challenge response, with the proper platform integrity metric, which it extracts from the certificate.', of Chen, emphasis added);

comparing said first set of integrity information with said second set of integrity information (see column 11, lines 5-16 of Chen); and

generating said attestation value in accordance with said comparison (see column 11, lines 5-16 of Chen).

Referring to claim 4:

Chen, Nakayama, and Hino teach the claimed subject matter: a method for performing dynamic attestation (see claim 1 above). Chen further discloses the encryption key (see column 4, lines 56-58 of Chen).

Referring to claims 5, 19:

Chen, Nakayama, and Hino teach the claimed subject matter: a method for performing dynamic attestation (see claim 1 above). Chen further discloses the authentication (see column 7, lines 21-26 of Chen).

Referring to claim 6:

Chen, Nakayama, and Hino teach the claimed subject matter: a method for performing dynamic attestation (see claim 1 above). Chen further discloses the decryption (see column 7, lines 21-26 of Chen).

Referring to claim 8:

Chen, Nakayama, and Hino teach the claimed subject matter: a method for performing dynamic attestation (see claim 7 above). Chen further discloses the first and the second process (see figure 5, 'trusted device', 'user' [i.e., smart card] of Chen).

Referring to claim 17:

Chen, Nakayama, and Hino teach the claimed subject matter: a method for performing dynamic attestation (see claim 15 above). Chen further discloses retrieving a second set of integrity information (see column 11, lines 5-16 '...with the proper platform integrity metric, which is extracts from the certificate.', of Chen).

Referring to claim 18:

Chen, Nakayama, and Hino teach the claimed subject matter: a method for performing dynamic attestation (see claim 15 above). Chen further discloses comparing the first set of integrity metric with the second set of integrity metric (see column 11, lines 5-16 'compares', of Chen).

Referring to claim 9:

i. Chen teaches:

A method, comprising:

a first processing comprising a plurality of applications and a first processor (see figure 5, elements 530, 535, 540; column 4, line 59-column 5, line 2; and column 11, lines 5-16 of Chen);

a second processing system to connect said first processing system , said second processing system comprising a second processor (see figure 5, element 'user' [i.e., smart card] of Chen); and

a dynamic attestation module to connect to said first and second processing systems, said second processing system to perform dynamic attestation for one of said applications to be executed by said first processing system using said dynamic attestation module, wherein said dynamic attestation module comprises an

integrity module to dynamically generate a first set of integrity information for said application by generating said first set of integrity information for said application using a cryptographic algorithm system prior to execution of said application by said first processing system (see column 11, lines 5-16, '...compares the computed integrity metrics, which it extracts from the challenge response, with the proper platform integrity metric, which it extracts from the certificate.'; and figure 5, element 590 'establish secure communication', of Chen, emphasis added).

However, Chen does not specifically mention the antenna and the transceiver.

Chen discloses dynamic authentication of the platform and application (see column 8, lines 4-16, particularly "Other know processes, for example virus checkers, will typically be in place to check that the operating system and **application program** code has not been subverted", of Chen, emphasis added). However, Chen does not specifically mention selecting an application from a plurality of applications.

Chen discloses generating set of integrity information for a processing system during boot operation (see column 7, lines 19-21 'During the secure boot process, the trusted device 24 acquires an integrity metric of the computing platform 10.', of Chen). However, Chen does not specifically mention the processing system that has completed trusted boot operation to verify integrity of an application prior to execution of the application.

Chen discloses terminating the session by the trusted device in case of an error or failure occurs (see column 13, lines 30-31, of Chen). However, Chen does not specifically mention disabling access by the processing system to a transceiver of the device.

ii. Nakayama teaches a portable terminal wherein Nakayama discloses the antenna and the transceiver for communicating with other servers (see figure 3, element 'A' [i.e., antenna]; and figure 11, elements 23 'application receiver', element 27 'value entity transmitter', of Nakayama).

Nakayama further discloses selecting an application from a plurality of applications (see figure 5, element 222 'service identifier area' [i.e., a plurality of applications]; page 7, paragraph [0102], lines 9-12 "The service identifier area 222 stores identifiers of services (e.g., "0001", "0002", "0003",...) for which the corresponding value entities in the value entity area 221 are used"; and paragraph [0098], lines 7-9 "or pull-type transmission in which the store server 30 transmits the application in response to an active transmission request from the portable terminal 20", of Nakayama).

On the other hand, Hino teaches a authentication system wherein Hino discloses the processing system that has completed trusted boot operation to verify integrity of an application prior to execution of the application (see column 2, lines 5-11 'Authentication may be performed during any period when inoperativeness of unauthenticated programs is guaranteed. Therefore, the authenticator accepting period is not limited to a boot period which will be described below. That is, authentication is not limited within a period starting from generation of a system reset, and not limited within a period ending at activation of an OS.'; and column 3, lines 37-59, of Hino, emphasis added).

Hino further discloses a hardware having a disabling and an enabling functionality (see column 3, lines 60-63, of Hino).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Nakayama into the method of Chen to use an antenna and a transceiver for communicating with other servers.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Nakayama into the method of Chen to select an application from a plurality of applications for authentication.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Hino into the method of Chen to use the processing system that has completed trusted boot operation to verify integrity of an application prior to execution of the application.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Nakayama into the system of Chen to use an antenna and a transceiver, because Chen teaches a method for performing dynamic attestation via integrity metric (see claim 1 above), and Nakayama teaches utilizing integrity measurement in a portable terminal (see e.g. figure 11, element 20 'integrity measurement part' of Nakayama). Therefore, Nakayama's teaching could enhance Chen's teaching by expanding Chen's method for performing dynamic attestation into a portable device.

The ordinary skilled person would have been motivated to have applied the teaching of Nakayama into the system of Chen to select an application from a plurality of applications for authentication, because Chen teaches dynamic authentication of platform and applications (see column 8, lines 4-16 of Chen), and Nakayama teaches selection an application from a plurality of applications (see ii). Therefore, Nakayama's teaching could enhance Chen's system by providing flexibility.

The ordinary skilled person would have been motivated to have applied the teaching of Hino into the system of Chen to use the processing system that has completed trusted boot operation to verify integrity of an application prior to execution of the application, because Chen teaches dynamic authentication of platform and applications (see column 8, lines 4-16 of Chen), and Hino teaches using the processing system that has completed trusted boot operation to verify integrity of an application prior to execution of the application. Therefore, Hino's teaching could enhance Chen's system by providing security.

Referring to claims 11:

Chen, Nakayama, and Hino teach the claimed subject matter: a method for performing dynamic attestation (see claim 9 above). They further disclose retrieving a second set of integrity information (see column 11, lines 5-16 '...with the proper platform integrity metric, which is extracts from the certificate.', of Chen).

Referring to claims 12:

Chen, Nakayama, and Hino teach the claimed subject matter: a method for performing dynamic attestation (see claim 9 above). They further disclose

comparing the first set of integrity metric with the second set of integrity metric (see column 11, lines 5-16 'compares', of Chen).

Referring to claims 13:

Chen, Nakayama, and Hino teach the claimed subject matter: a method for performing dynamic attestation (see claim 9 above). They further disclose the authentication (see column 7, lines 21-26 of Chen).

Referring to claims 14:

Chen, Nakayama, and Hino teach the claimed subject matter: a method for performing dynamic attestation (see claim 9 above). They further disclose disabling access (see column 3, lines 60-67, of Hino).

Response to Arguments

4. Applicant's arguments, filed on October 7, 2009, have been fully considered but they are not persuasive.

(a) Applicant argues:

"Applicant respectfully submits that claim 1 defines over Hino because Hino fails to disclose, teach or suggest at least the second processing system disabling access by the first processing system to a transceiver of the device if the integrity of the application is not verified." (see page 9, 2nd paragraph)

Examiner maintains:

Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chen in view of Nakayama and further in view of Hino.

Chen discloses "In step 540, the user receives the challenge response and verifies the certificate using the well known public key of the TP. The user then, in step 550, extracts the trusted device's 24 public key from the certificate and uses it to decrypt the signed digest from the challenge response. Then, in step 560, the user verifies the nonce inside the challenge response. Next, in step 570, the user compares the

computed integrity metric [i.e., verifying the integrity of the application], which it extracts from the challenge response, with the proper platform integrity metric, which it extracts from the certificate. If any of the foregoing verification steps fails [i.e., if the verification fails], in steps 545, 555, 565 or 575, the whole process ends in step 580 with no further communications taking place [i.e., disabling the transceiver in step 580 with no further communications taking place]." (see column, lines 5-16, of Chen, emphasis added).

Therefore, Chen discloses the second processing system ending [i.e., disabling] access by the first processing system to a transceiver of the device if the integrity of the application is not verified. However, Chen does not explicitly use the term "disable".

On the other hand, Hino discloses "Preferably, the program executing means has hardware, the hardware having a function of **enabling** and **disabling** transmission of an electric signal of the authenticator of the program executing means from the program executing means, and the hardware further enabling the program executing means to transmit the electric signal of the authenticator of the program executing means from the point of initial detection of a system reset signal." (see column 3, lines 60-67, of Hino, emphasis added). Therefore, Hino discloses the hardware having a function of enabling and disabling a transmission of a electric signal.

Thus, the combination of references disclose the second processing system disabling access by the first processing system to a transceiver of the device if the integrity of the application is not verified, such as discloses in the claimed invention.

(b) Applicant argues:

"Furthermore, Chen does not teach a second processing system, comprising a second processor of a device, disabling access by a first processing system, comprising a first processor of the device, to a transceiver" (see page 9, 3rd paragraph)

Examiner maintains:

The combination of references disclose the second processing system disabling access by the first processing system to a transceiver of the device if the integrity of the application is not verified (see (a) above).

Chen further discloses "FIG. 5 illustrates the flow of actions by a TP, the trusted device 24 [i.e., the first processing system comprising the first processor of a device] incorporated into a platform [i.e., the device], and a user (of a remote platform) who wants to verify the integrity of the trusted platform. It will be appreciated that substantially the same steps as are depicted in FIG. 5 are involved when the user is a local user. In either case, the user would typically rely on some form of software application to enact the verification. It would be possible to run the software application on the remote platform or the trusted platform. However, there is a chance that, even on the remote platform, the software application could be subverted in some way. Therefore, it is anticipated that, for a high level of integrity, the software application would reside on a smart card of the user, who would insert the smart card [i.e., the second processing system comprising the second processor of the device] into an appropriate reader for the purposes of verification." (see column 9, line 65 to column 10, line 12, of Chen, emphasis added).

Therefore, the references disclose a second processing system, comprising a second processor of a device, disabling access by a first processing system, comprising a first processor of the device, to a transceiver, such as claimed.

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Joseph Pan/
Examiner, Art Unit 2435
December 15, 2009

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435